

SECURE AND ROBUST QR CODE EMBEDDED IN MEDICAL IMAGE USING SSIM and MS-SSIM

Mr.N.Senthilnathan¹

¹Department of ECE
AnnaUniversity,BITCampus,
Tiruchirappalli,Tamilnadu,India.

Dr.A.Adaikalam²

Department of ECE
AnnaUniversity,BITCampus,
Tiruchirappalli,Tamilnadu,India.

Abstract

Two main techniques used for information secure transmission in internet are cryptography and steganography. Now days the Quick Response (QR) codes have been widely used in important applications such as data storage and high-speed machine reading in information security. The drawback of information stored in QR codes to access the encoding secret information without using any cryptography protection security system. In this proposed paper used structural similarity (SSIM) index method for measuring the similarity between two images to encode a secure and robust QR code embedded into medical image and new medical image-embedding 2D barcode, which mitigates these two limitations by equipping a non-scannable 2D barcode with a medical image picture sequence appearance. Proposed of this work for text security and also improve the mean and standard deviation value in embedded image using Structural Similarity Index Measuring (SSIM) and Multiscale Structural Similarity Index Measuring (MS-SSIM) technique. The medical QR code has been simulated in MATLAB using different format and size of images. Simulation result shows that the proposed SVD give better performance improved in terms of patient information

securely and improved visual secret sharing over the existing secure technique.

Keywords: Quick Response (QR), structural similarity (SSIM) index method, Multiscale Structural Similarity Index Measuring (MS-SSIM) and with singular value decomposition (SVD).

1. INTRODUCTION

The data's are transferred through internet in various formats like text, video, graphics objects and audio. In multimedia communication, the data exchanging is insecure and unreliable. The most popular protection security systems like cryptography techniques are used in data transfers. In cryptography, the data's are converted into cipher using well known algorithms, for example, RSA, AES and ECC. The above cited algorithms are used to encrypt the text data's only. There is need to secure the image transmission, Even though steganography method is used to transfer the image in a secure manner. But still big data transmission needs novel methods, therefore this

article presents the novel method called Visual Cryptography (VC). In this proposed method, the private key (k,n) has been used to protect images contents. Where 'k' is any shares or content and 'n' is the number of shares using logical operators either AND or OR to find the original secret image. The advantage of VC is no mathematical, computational calculation in multimedia data transmission with secret image.

In past years, confirmed security without substantial computation using the human visual system and visual secrete scheme. In 'k' out of 'n' accurate cipher text in cryptography, which means allocating the information of secrete into a multiple number of looking shares in a random manner. So, that minimum number of k-shares requires to retrieving the original secret image. The visual secrete scheme mainly using codebook, which contains each pixel encoded by two sub pixels represented by either 0 is black pixel or white pixel is 1. The pixel configuration issues are recovered secret due to contrast loss and misalignment of random shares issues is reduce must design codebook, detecting individual share and cannot identify whether the secret pixel either white or black.

In existing OR visual secrete scheme various issues like resolution, contrast and colour image over the XOR based secret

scheme. It is more advanced as one of the probable solutions, especially above mention issues and advantage of XOR based VC scheme was the extermination of pixel alignment problem existing in visual cryptography method. Decryption of the secret image from the shares can be retrieved using less computational devices in an XOR using VC method. The recovered secret image improved in the contrast 50 % using OR-based VC method. The issues of XOR based scheme are codebook construction and separate shares obtained without meaning is reduce the contrast of the recovered images with existing of pixel expansion and random shares pattern. The random share problem was resolute by introduction of significant shares based on n out of n XOR based visual scheme. But the result is poor visual quality in the recovered meaningful shares and secret image issues are solved.

The following section 2 is consisting of related work, section 3 contains the detail of proposed work and section 4 illustrated results and performance. Finally, conclusion and references are given.

2. RELATED WORK

The author [1] examine secret sharing method encrypting audio secrets, the result of the encryption uses random variable sampled over a normal boundary condition. This result

increases the increase in the computation and confidence of the cryptography system. The proposed article [2] provide visual secret sharing schemes encryption multiple image by formulation of VSS encryption.

The Javvaji et al. [3] provide high security to the secret image by simple Boolean XOR and circular shift operation; in this proposed technique result provide to increase the security of the original secret image to great extended image to make more flexible and adoptable with high security. The author [4] examined two variant of secrete sharing scheme to increase the security by using XOR and Gray code operation. In this operation there is no information loss used encrypted scheme along with secrete key.

Her-Chang choo [5] discussed visual secret sharing using generalized random grids. In this scheme decrypting the recover the original image with an XOR operator produce secret image with high quality and there is no pixel expansion of the sharing secret image, without using any codebook over the existing scheme. In this [6] proposed method to highly security and hiding capacity is improved by using steganography method PNG image, which used multiple layer to hide the data. In this proposed scheme obtained high PSNR value compare with existing method Substitute last

digit in pixel (SLDIP) and Modified Substitute last digit in pixel (MSLDIP) which is highly suggested as the security concern for video data hiding. The proposed [7] design of algorithm for text hiding security using improve the PSNR and MSE value to obtain the best qualitative and quantitative analysis report. Based on the result the proposed technique can hide the date approximately 16KB and 260KB cover image of size is 128 x 128 and 800 x 800 pixel compare the existing algorithm result.

In [8] developed new algorithm for generation of random share basic matrices to meet out the objective of this proposed visual cryptography secure system. Based on the comparative result of existing approaches it's improving the efficiency of the proposed algorithm by requirement of codebook and lossless of improved secret image. The author [9] present scheme is different from the conventional scheme based on new password authentication protocol in image. The image are encoded by VC with OCR number, It will provide high secure from cyber-attack. The proposed [10] novel algorithm of robust visual secret sharing scheme using Quick Response (QR) code function is first all the code word of the secret QR code image are encoded and decoded in to temporary binary QR code image and standard QR decoder. The secret image can be recover by XOR operation and the original

text was identical recovered so, the effectiveness of proposed scheme used in wireless multimedia security application by the experimental result.

3.PROPOSED WORK

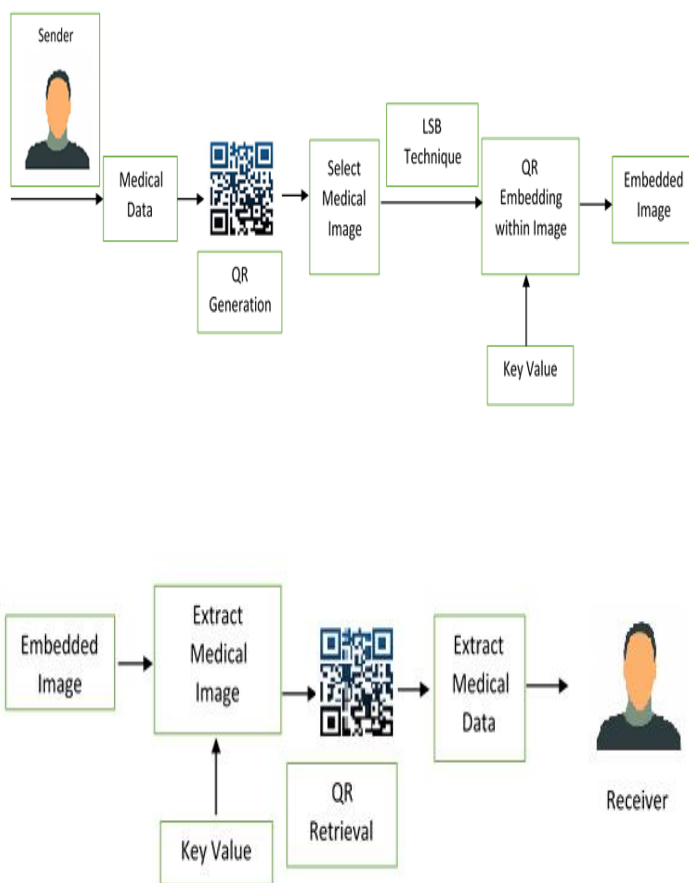


Figure.1. System Architecture (Encryption and Decryption)

Procedure:

3.1 Medical Data Hidden within QR code

The figure 1 show the system architecture of both encryption and decryption

process of text hiding, it is a process of embedding the secret text imperceptibly into the cover media by minimally modifying the elements of the cover media. In this module sender will upload medical data for transmit to the receiver. Medical data is present in the form of normal text in English words. Uploaded texts message was converted into QR format. QR is a quick response code that will be generated to provide secure to the medical data.

3.2 Image Upload

This process is to select cover media for information hiding. Here images are used as a cover media for the secret message. Cover image is also select by the sender when create the secret message. Original message is hidden into the cover media (image) to improve the security of data sharing. The steganography image that has to send should be uploaded. The image should be any one of the image supporting formats. The various supporting formats are JPEG, PNG & BMP. A text is written and hidden inside a secret image. This is done by using LSB method. The cover image is called as a steganography image is shown figure 3.

3.3 Image Encryption

Steganography image will be encrypted separately using XOR operation. A key is used to encrypt the shares. Exclusive-or encryption requires that both encryption and decryption

have access to the encryption key, but the encryption algorithm, while extremely simple, is nearly unbreakable. That key will be mailed to the receiver. If JPEG image is used, the encrypted share will be in black and white colour. It will look like a QR code. By using this module, the encrypted image will be sent to the receiver. This will help to avoid the information loss and also it saves transmission and receiving time for both sender and receiver.

3.4 Image Decryption

The encrypted image will be received by the receiver in a single transmission. Each received share will be decrypted individually using inverse XOR method and experimental output of medical QR code are shown in figure 2, figure 4 and figure 5. The output of this module will be an steganography image in decrypted form. The recovered image can be viewed as a complete single image. Finally, the original input image and output recovered image dimension is same which is shown in figure 6.

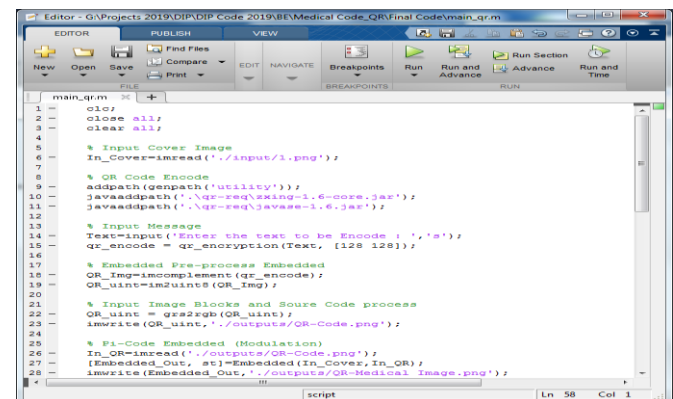
3.5 Recovered QR code and Medical Data

In this module receiver can retrieve QR code and text. After decryption image receiver can extract QR based text. Data extraction is the process of extracting the original data. The hidden text will be recovered from the secret image is shown figure 7. Receiver gets the secret message with cover text using LSB

method, which is used to retrieve the hidden text. Specific key, is generated and shared to the receiver during the process of message sending. Receiver can decrypt the text is shown in figure 8 using shared secret key. Then the original message is shown to the receiver.

4. RESULT AND PERFORMANCE

The procedure for experimental output of medical QR code are shown in figures 2, 4 and 5



```

1 - clear;
2 - close all;
3 - clear all;
4
5 % Input Cover Image
6 In_Cover=imread('input/1.png');
7
8 % QR Code Encode
9 addpath(genpath('utility'));
10 javaaddpath('..\qr-req\sking-1.6-core.jar');
11 javaaddpath('..\qr-req\javage-1.6.jar');
12
13 % Input Message
14 Text=input('Enter the text to be Encode : ','s');
15 qr_encode = qr_encryption(Text, [28 28]);
16
17 % Embedded Pre-process Embedded
18 In_Img=imcomplement(qr_encode);
19 QR_uint=uint8(In_Img);
20
21 % Input Image Blocks and Source Code process
22 QR_uint = qrs2rgb(QR_uint);
23 imwrite(QR_uint, './outputs/QR-Code.png');
24
25 % FI-Code Embedded (Modulation)
26 In_OR=imread('./outputs/QR-Code.png');
27 [Embedded_Out, at]=Embedded(In_Cover, In_OR);
28 imwrite(Embedded_Out, './outputs/QR-Medical Image.png');

```

Fig. 2. Experimental result of Medical QR Code

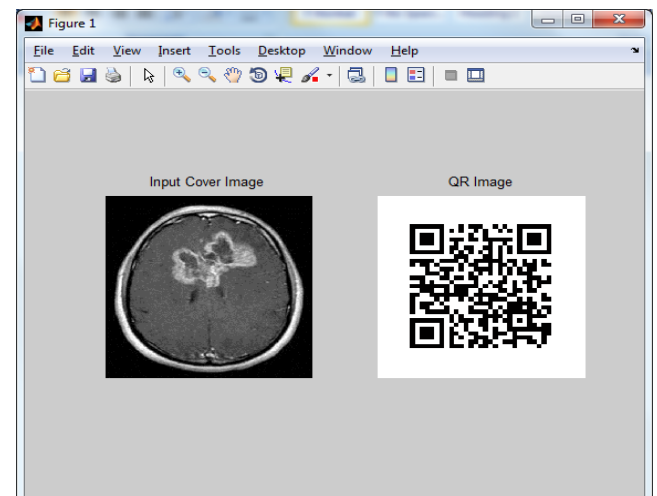


Fig.3. Input Cover Image 512 x 512 with QR code Reclamation

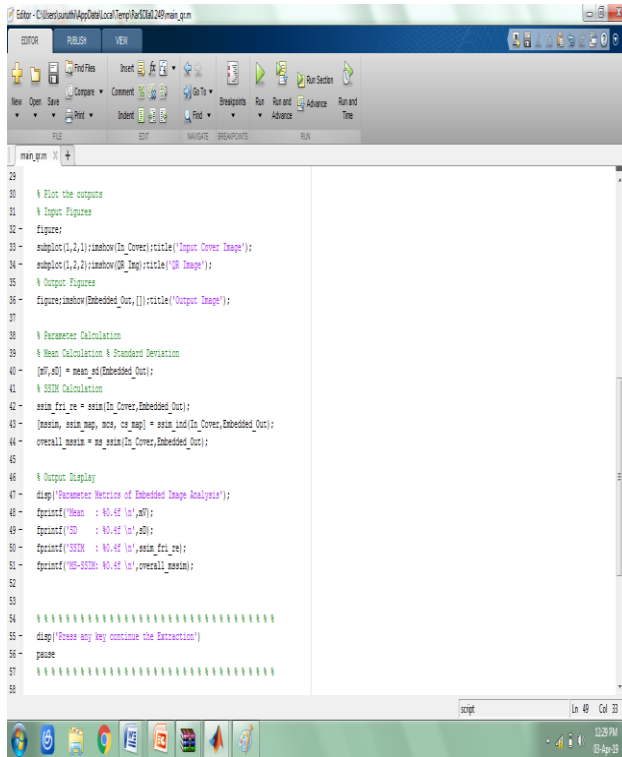


Fig.4. Experimental result of Medical QR Code

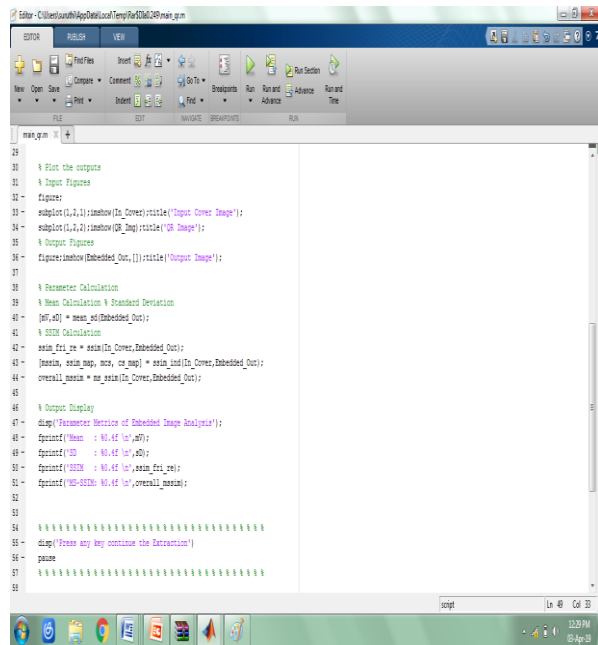


Fig.5. Experimental result of Medical QR Code

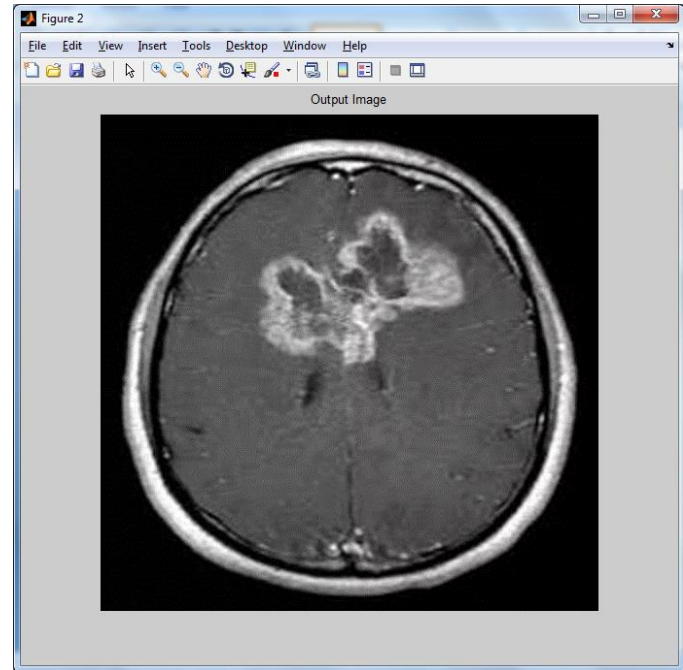


Fig.6. Experimental result of Output Embedded Image

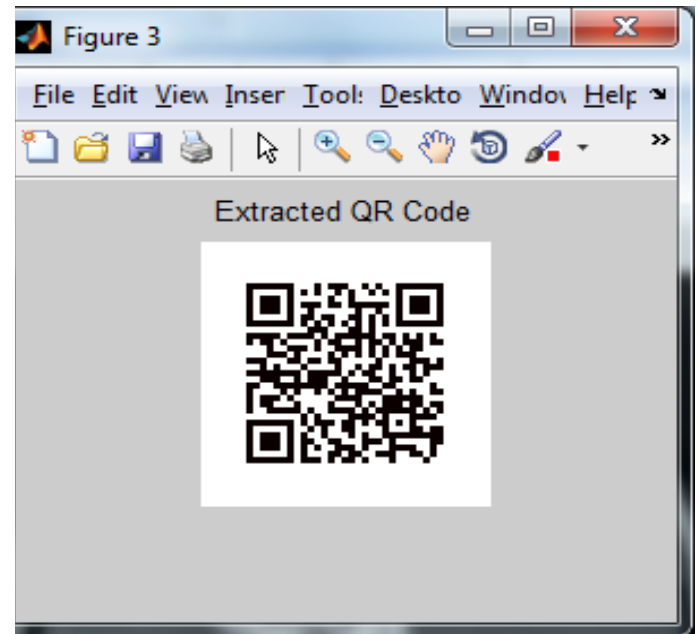


Fig.7. Extract QR Code

Table 1: Comparison of mean and standard deviation value in embedded images of visual cryptography scheme with singular value decomposition (SVD).

| Input Image with QR Code Embedded | | Existing System Used in Visual cryptography scheme | Proposed System Used in singular value decomposition Technique |
|-----------------------------------|---------|---|---|
| Mean (μ) | Image 1 | 0.2105 | 0.3067 |
| | Image 2 | 0.3235 | 0.3249 |
| | Image 3 | 0.4158 | 0.5120 |
| Standard Deviation (σ) | Image 1 | 0.2871 | 0.4749 |
| | Image 2 | 0.0058 | 0.3697 |
| | Image 3 | 0.3122 | 0.3945 |

```

Command Window
Enter the text to be Encode : Name:Alpha DOB: 1-2-1990 Blood Group: o+ve
Parameter Metrics of Embedded Image Analysis
Mean : 0.3066
SD : 0.4749
SSIM : 0.9895
MS-SSIM: 1.0000
Press any key continue the Extraction
Decrypted text from the QR: Name:Alpha DOB: 1-2-1990 Blood Group: o+ve
fx >>
    
```

Fig.8.QR Decrypted Text

The mean and standard values are embedded in different images are described table 1 using visual cryptography and single singular value decomposition scheme and table 2 shown the SSIM and MS-SSIM embedded images compare the proposed SVD scheme.

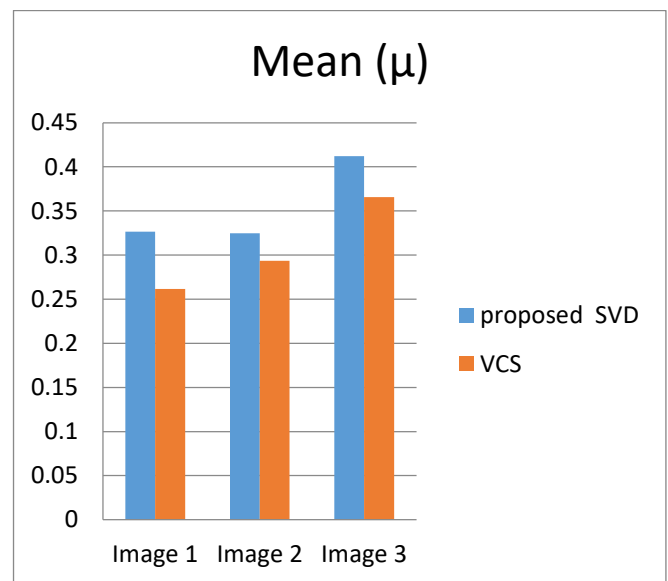


Figure 8 a: Comparison of mean value in embedded with images of visual cryptography scheme with singular value decomposition (SVD)

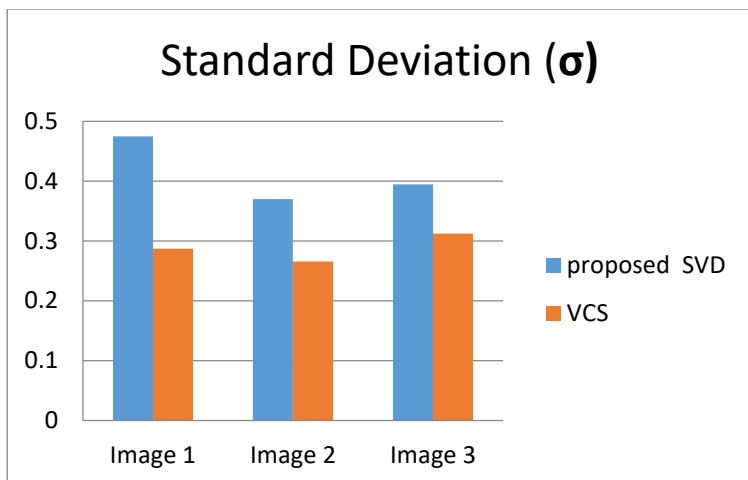


Figure 8 b: Comparison of standard deviation value in embedded images of visual cryptography scheme with singular value decomposition (SVD)

Table 2: comparison of SSIM and MS-SSIM in embedded images of visual cryptography scheme with singular value decomposition (SVD)

| Input Image with QR Code Embedded | | Existing System Used in Visual cryptography scheme | Proposed System Used in singular value decomposition Technique |
|-----------------------------------|---------|---|--|
| SSIM | Image 1 | 0.8743 | 0.9890 |
| | Image 2 | 0.9214 | 0.9941 |
| | Image 3 | 0.9645 | 0.9875 |
| MS-SSIM | Image 1 | 0.2871 | 0.4749 |
| | Image 2 | 0.0058 | 0.3697 |
| | Image 3 | 0.0185 | 0.2151 |

The secure information is computed to improve the value of mean and standard deviation for different embedded image. The comparison of SSIM and MS-SSIM in embedded images of visual cryptography scheme with singular value decomposition (SVD) is shown in Figure 9.

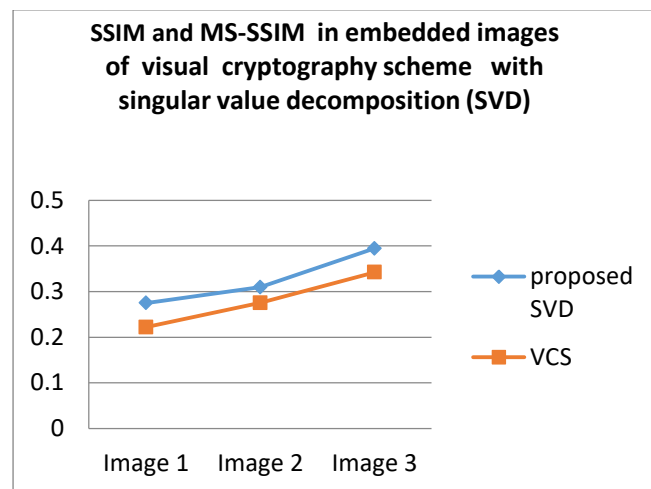


Figure 9: comparison of SSIM and MS-SSIM in embedded images of visual cryptography scheme with singular value decomposition (SVD)

5. Conclusion

Based on the discussion of the various analytical simulation results comparing with the performance of the existing visual cryptography scheme. The information stored in QR codes to access the encoding secret information without using any cryptography protection security system avoid this to improve the mean and standard deviation of experimental three images mean value results are 0.35, 0.36 and 4.1 and standard deviation is 0.47, 0.36 and 0.39 is shown in figure 8a and 8b and the result is improve the securely information

from 0.25 to 0.40 % visual secret sharing over the existing secure technique is shown in figure 9. It is concluded that the use of proposed SVD reduces the save more memory space and securely patient information etc.,

6. Reference

- [1] Washio, Shinya, and Yodai Watanabe. "Security of audio secret sharing scheme encrypting audio secrets with bounded shares." In 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 7396-7400. IEEE, 2014.
- [2] Sasaki, Manami, and Yodai Watanabe. "Formulation of visual secret sharing schemes encrypting multiple images." In 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 7391-7395. IEEE, 2014.
- [3] Ratnam, Javvaji VK, P. Ramana Reddy, and T. Sreenivasulu Reddy. "Design of high secure visual secret sharing scheme for gray scale images." In 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 145-148. IEEE, 2017.
- [4] Deepika, M. P., and A. Sreekumar. "Secret sharing scheme using gray code and XOR operation." In 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1-5. IEEE, 2017.
- [5] Chao, Her-Chang, and Tzuo-Yau Fan. "XOR-based progressive visual secret sharing using generalized random grids." *Displays* 49 (2017): 6-15.
- [6] Teja, Jyothula Dharma, A. Chandra Sekhara Rao and Suresh Dara, "A New Image Steganography Technique for Hiding the Data in Multi Layers of the PNG Images", *Int. J. Ad Hoc and Ubiquitous Computing* 10, no. Y4 (2017).
- [7] Chauhan, Shivani, Janmejai Kumar, and Amit Doegar. "Multiple layer text security using variable block size cryptography and image steganography." In 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), pp. 1-7. IEEE, 2017.
- [8] Singh, Priyanka, Balasubramanian Raman, and Manoj Misra. "A (n, n) threshold non-expandable XOR based visual cryptography with unique meaningful shares." *Signal Processing* 142 (2018): 301-319.
- [9] Chen, Yu-Chi. "Fully incrementing visual cryptography from a succinct non-

monotonic structure." IEEE Transactions on Information Forensics and Security 12, no. 5 (2017): 1082-1091.

- [10] Longdan.T, Kesheng.L, Xuehu.Y, Lintao.L, Tianqi .L, Jinrui.C, Feng.L, and Yuliang .L, "Robust Visual Secret Sharing Scheme Applying to QR Code, Security and Communication Networks Vol. 2018,pp. 1-12,2018.